IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application for:

RECONSTITUTION OF PROGRAM STREAMS SPLIT ACROSS MULTIPLE PROGRAM IDENTIFIERS

Inventor(s): Robert Unger

Docket Number: SNY-R4976

Prepared By: Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606

Phone: (919) 816-9981
Fax: (919) 816-9982
Email: miller@patent-inventions.com

CERTIFICATE OF EXPRESS MAILING FOR NEW PATENT APPLICATION

"Express Mail" mailing label number EK555545385US

Date of Deposit 2/27/2002

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Jerry A. Miller
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

RECONSTITUTION OF PROGRAM STREAMS SPLIT ACROSS MULTIPLE PROGRAM IDENTIFIERS

CROSS REFERENCE TO RELATED DOCUMENTS

This application is related to U.S. provisional patent application serial number 60/296,673 filed June 6, 2001 to Candelore, et al. entitled "Method for Allowing Multiple CA Providers to Interoperate in a Content Delivery System by Sending Video in the Clear for Some Content, and Dual Carriage of Audio and Dual Carriage of Video and Audio for Other Content", and provisional patent application serial number 60/304,241 filed July 10, 2001 to Unger et al., entitled "Independent Selective Encryptions of Program Content for Dual Carriage", and provisional patent application serial number 60/304,131 filed July 10, 2001 to Candelore et al., entitled "Method for Allowing Multiple CA Providers to Interoperate in a Content Delivery System by Partial Scrambling Content on a Time Slice Basis" and to U.S. provisional patent application serial no. 60/343,710, filed on October 26, 2001 to Candelore et al., entitled "Television Encryption Systems", docket number SNY-R4646P, which are hereby incorporated herein by reference.

This application is also related to patent applications docket number SNY-R4646.01 entitled "Critical Packet Partial Encryption" to Unger et al., serial number 10/038,217; patent applications docket number SNY-R4646.02 entitled "Time Division Partial Encryption" to Candelore et al., serial number 10/038,032; docket

number SNY-R4646.03 entitled "Elementary Stream Partial Encryption" to Candelore , serial number 10/037,914; docket number SNY-R4646.04 entitled "Partial Encryption and PID Mapping" to Unger et al., serial number 10/037,499; and docket number SNY-R4646.05 entitled "Decoding and Decrypting of Partially Encrypted Information" to Unger et al., serial number 10/037,498. These patent applications were filed simultaneously on January 2, 2002 and are hereby incorporated by reference herein.

COPYRIGHT NOTICE

FIELD OF THE INVENTION

This invention relates generally to the field of multiply encoded program data streams identified by multiple program identifiers (PIDs). More particularly, in certain embodiments, this invention relates to reconstitution of multiple encrypted multiple carriage program data streams.

BACKGROUND OF THE INVENTION

Several different and incompatible encryption systems are currently in use in cable television systems. In general, each encryption system is specific to a particular manufacturer and is maintained as a proprietary system. When a cable system operator (or other content distributor) builds a system around a particular manufacturer, it becomes difficult and expensive to change to another manufacturer that may provide lower cost or higher performance hardware. Thus, a content

distributor is often locked into a single source of hardware (e.g., television set-top boxes).

This problem can be avoided somewhat by using a technique known as "dual carriage" (or "multiple carriage")of encrypted content. In this technique, the same program is duplicated with each copy sent with a different type of encryption. Thus, multiple set-top boxes from multiple manufacturers can coexist on the same system. Unfortunately, this technique has a serious bandwidth penalty due to the need to transmit duplicate copies of all content.

The above-referenced patent applications describe techniques referred to as "partial encryption" or "selective encryption". These techniques are used to effectively permit a virtual form of "dual carriage" (or multiple carriage) of a television program over a single distribution system (e.g., a cable television system) using multiple encryption techniques. By only partially encrypting a particular program (i.e., only encrypting certain portions of the digital data associated with a program), multiple copies of the encrypted portion of the program can be carried over the distribution system with the remaining content carried in the clear. These techniques permit a virtual form of dual carriage (or multiple carriage) of the program content with a minimal bandwidth penalty. A significant advantage of such a system is that the content provider (e.g., a cable television system operator) can use television set-top boxes (STBs) provided by multiple manufacturers that encrypt content under multiple encryption systems without suffering a large bandwidth penalty.

In a conventional cable system, system information (SI) is provided in the form illustrated in **FIGURE 1** of a Program Association Table (PAT) which contains an entry for each program. Each program in the PAT has a pointer to a particular Program Map Table (PMT) such as 12, 14, ... 18 and 20 associated with the particular program. The PMT table contains Program Identifiers (PIDs) that are associated with the elementary streams for each program.

In the above-referenced patent applications, the multiple sets of encrypted packets representing the encrypted portions of the partially encrypted programs are

distinguished from one another by use of distinctive program identifiers (PIDs). Thus, for example, two encrypted portions of a program have two unique PIDs - a primary PID and a shadow (or secondary) PID. In order for the receiving equipment to determine which PIDs are associated with a particular encryption scheme, the PID information is transmitted from the cable system (or other distributor) headend. In one embodiment, illustrated in **FIGURE 2**, this can be done using a duplicate set of system information (SI) to identify the various PIDs. In this example, two separate PATs 30a and 30b are used to associate programs with PATs 32a, 34a, ...38a and 40a in the case of PAT 30a, and with 32b, 34b,...38b and 40b in the case of PAT 30b. Each receiving system is able to detect and process whichever SI is appropriate. The system (e.g., the cable system headend) generating the SI creates duplicate SI for each encryption scheme used. When bandwidth is critical, the extra packets used to transmit the duplicate SI may be difficult to accommodate.

Systems that are aware that shadow PIDs exist need to know of the PID pairs and reconstitute the merged stream. The system then needs a method to reconstitute the shadow stream from the payloads of both PIDs.

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the invention believed to be novel are set forth with particularity in the appended claims. The invention itself however, both as to organization and method of operation, together with objects and advantages thereof, may be best understood by reference to the following detailed description of the invention, which describes certain exemplary embodiments of the invention, taken in conjunction with the accompanying drawings in which:

FIGURE 1 depicts System Information as used in a conventional digital cable television system.

FIGURE 2 illustrates how a duplicate set of System Information could be used in a dual carriage environment.

FIGURE 3 illustrates System Information in accordance with certain embodiments of the present invention.

FIGURE 4 illustrates a television set-top box consistent with certain embodiments of the present invention.

FIGURE 5 illustrates the toggling of buffers in a manner consistent with certain embodiments of the present invention.

FIGURE 6 shows the proximal relationship of primary and shadow packets in certain embodiments of the present invention.

FIGURE 7 is a flow chart of the data buffering and interrupt generation consistent with certain embodiments of the present invention.

FIGURE 8 is a flow chart illustrating finding corresponding packets and reconstitution of a program data stream in accordance with certain embodiments of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

While this invention is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail specific embodiments, with the understanding that the present disclosure is to be considered as an example of the principles of the invention and not intended to limit the invention to the specific embodiments shown and described. In the description below, like reference numerals are used to describe the same, similar or corresponding parts in the several views of the drawings.

Turning now to **FIGURE 3**, according to certain embodiments of the invention, additional SI is provided using a technique that uses only a small amount (e.g., one packet in certain embodiments) of additional information per encryption scheme used (can be shared across several programs). The PAT 50 is again associated with a plurality of PMTs 52, 54,...58 and 60. Additional information is provided in the form of a translation table or lookup table 70 that translates between the primary PID used by the primary encryption scheme and the shadow

PID used as a shadow substitute. This lookup table 70 is provided as a private data packet. The rest of the SI tree structure remains as if only the primary encryption scheme existed.

In certain embodiments, the PAT contains the PID of the packet with the translation table as part of a user private data section. The translation table can contain data as indicated in **TABLE 1** below. The table data in the translation packet permits a lookup of each affected primary PID and its associated shadow PID. The receiving device (e.g. STB) uses this information to configure its PID filters and demultiplexers.

Primary PID	Shadow PID
Program 1 video	Shadow video of Program 1
Program 5 video	Shadow video of Program 5
Program 1 ECM	ECM to use with program 1
Program 5 ECM	ECM to use with program 5

TABLE 1

In utilizing this arrangement, the nominal PAT table is used to find the program of interest and the primary PIDs for that program. These primary PIDs are checked against the translation table to see if there is an associated shadow PID. If a video PID matches, then the stream reconstitution mechanism (hardware, firmware, software) is initialized with the two PIDs. If an ECM (Entitlement Control Message) PID matches, then the decryption circuit is initialized with the entitlement control message having the shadow PID instead of the primary PID.

In certain of the selective encryption arrangements described in the above-referenced patent applications, legacy receiver systems (e.g. set-top boxes) are

accommodated by dual encrypting certain packets. Programs destined for the legacy system contain unencrypted packets having a first PID and encrypted packets also having the first PID. Thus, the legacy system sees encrypted and unencrypted packets having the same PID and simply decrypts packets requiring decryption. The same encrypted packets having the primary PID are also duplicated and encrypted under a second encryption system and assigned the shadow PID. Thus, for a non-legacy system (e.g., non-legacy set-top boxes) using the second encryption technique, in order to have a data stream with all the information required to decode a particular program, the unencrypted data packets with the Primary PID are combined with data packets having the shadow PID to reconstitute the total program.

<u>Recostitution</u>

Once the receiver device, such as a television or television set-top box has the information used to map programs to primary and shadow PIDs, the program is reconstituted by decryption of the packets with shadow PIDs and inserting the decrypted packet into the data stream containing the unencrypted packets. In accordance with the selective encryption arrangements described in the above-referenced patent applications, data packets having shadow PIDs would commonly be received with significantly reduced frequency compared with data packets having primary PIDs. The current embodiment takes advantage of this relatively slow rate of shadow packet reception to reduce PID processing in a software implemented double buffer scheme as illustrated in **FIGURE 4**.

Not all implementations of selective encryption for virtual dual carriage can use existing hardware or firmware to implement stream reception in the set top box or other receiver. Buffering incoming data into memory in a conventional hardware facilitated (via DMA) double buffer scheme can be problematic. According to this scheme, when a buffer is full, an interrupt is generated, and the software toggles to the alternate fill buffer. Using this scheme to find packets with one or more particular PIDs, the received data in the filled buffer would then be scanned for the

PIDs of interest, and then the desired packet sequence would be rebuilt. Unfortunately, such a process might introduce an undesirable delivery latency and utilize an unnecessary amount of CPU processing power to process all packets received since differentiation is not performed until the buffer is full. This potential problem can be avoided using the arrangement of **FIGURE 4**.

The STB 100 of **FIGURE 4** has a packet demultiplexer 104 in the STB receiver front end that is programmed to generate an interrupt to the micro computer 110 when a packet with the shadow PID is detected and stored in the shadow packet buffers116. Primary packets are demultiplexed according to their PID at the demultiplexer 104 and sent to one of two primary packet buffers 120 and 122 in a typical toggled double buffer scheme. (A buffer pool with more than two buffers could work equally well.) Conceptually, for purposes of this explanation, the incoming data stream with the primary PID is sent to either buffer 120 or 122 based upon the position of micro computer 110 controlled switch 128 (of course, those skilled in the art will appreciate that such switching can be accomplished by addressing techniques and other equivalent methods known in the art).

Whenever a shadow packet is received and sent to buffer 116, the interrupt service routine toggles switch 128 to effectively change primary packet buffers at the shadow PID boundary. This limits the range of primary packets that the software must search in order to find the packet to be replaced by the shadow packet. Depending upon whether the headend places the shadow packet in the data stream just prior to or just after the corresponding encrypted packet having the primary PID, the corresponding packet can be found either at the end one primary packet buffer or the beginning of the other. Latency impacts are minimized since processing occurs within very few packet times and processing bandwidth is minimized since only one or two packets must be scanned by software to identify the correct packet.

This operation is illustrated in **FIGURE 5** in which primary packets are being loaded into primary packet buffer 120. When an interrupt is generated, by virtue of

the receipt of a packet with the appropriate shadow PID, the buffers are toggled so that data is now being loaded into primary packet buffer 122. In the ideal case where the buffers can be switched as a result of the receipt of a packet with the shadow PID instantaneously with no disruption of receipt of packets having primary PIDs, the incoming data stream will have had the packet with the shadow PID situated between primary packets N and N+1 as shown in **FIGURE 6**.

In this illustration, shadow packet 130 is situated between primary packet N 134 and primary packet N+1 138. The system headend can theoretically operate in any of three ways. Either the headend can always insert the shadow packet after its corresponding primary packet, before its corresponding primary packet or some combination thereof. (The term "corresponding" as used in this context is intended to mean packets that originated from the same packet of information. In this example, one packet is encrypted under a first encryption technique and the other is encrypted under a second encryption technique. One is assigned a primary PID and one is assigned a shadow PID. They are corresponding in that they ultimately carry the same payload once unencrypted.)

Once the buffers are toggled, in this ideal scenario, since the desired corresponding packet is situated adjacent the shadow packet 130, it is known that the corresponding packet is one of the packets 134 and 138. In the case where the shadow packet always precedes its corresponding primary packet, the corresponding primary packet is the first stored in the currently active (buffer 122 in the example shown in **FIGURE 5**). In the case of the shadow packet always following its corresponding primary packet, the corresponding primary packet is always the last packet stored in the inactive buffer (buffer 120 in the example shown in **FIGURE 5**). When it is unknown whether the shadow packet follows or precedes its corresponding primary packet, the determination is still easily made by inspecting at most the first packet in the active buffer and the last packet in the inactive buffer. Thus, in this embodiment, searching an entire buffer or other large quantity of data for a corresponding packet is reduced to searching at most one or

two packets. The packets can be confirmed as being corresponding packets in a number of ways, for example, corresponding packets may have the same packet sequence number, and the corresponding packets are both flagged as encrypted.

In some cases the software might not be able to change the DMA control registers without danger of a race condition. This can be addressed using an equivalent technique of logging the state of the DMA control registers when the shadow packet interrupt occurs. When the primary buffer is filled, the logged data can be used to find the location of the primary packet corresponding to the shadow packet.

Thus, a method of constructing a stream of data packets having primary and shadow packet identifiers (PIDs), the packets having headers and payloads consistent with certain embodiments of this invention include receiving an incoming data stream having packets with the primary and shadow PIDs; providing a stream of packets having the primary PID to a first buffer; detecting a packet having the shadow PID and a shadow payload in the incoming data stream; switching the stream of packets having the primary PID to a second buffer in response to the detecting; and searching a first packet stored in the second buffer and a last packet stored in the first buffer for a packet corresponding to the packet having the shadow PID.

Once a pair of corresponding packets are identified, the data stream belonging to a particular program can be reconstituted. This is ultimately done by creating a stream of unencrypted packets with the same PID. Thus, the corresponding primary packet can be modified by swapping the payload from the secondary packet into the corresponding primary packet, or by swapping the PID of the shadow packet to the primary PID and inserting it into the data stream. This selectively encrypted data stream can then be decrypted (where required) and decoded at 160 to produce a decoded digital television program (or other content).

The above process of buffering data and interrupt generation is shown in the flow chart of **FIGURE 7** starting at 200. As new data are received at 204, the data packets are inspected to determine if they have the shadow PID (i.e., to determine

if a shadow packet has been received) at 208. If not, and the packet is a primary packet, the primary packet is placed in which ever primary data packet buffer is currently active (120 or 122) at 212. However, if a shadow PID is detected at 208, an interrupt is generated at the demultiplexer at 218. This interrupt causes the active and inactive primary packet buffers to toggle at 222 (changing the inactive buffer to active and vice versa). Newly received primary packets are then placed in the active buffer at 212. Data in the just closed buffer is passed to the consuming device.

FIGURE 8 depicts the packet processing to reconstitute the program's data stream starting at 300. At 304, if no interrupt is detected, the process awaits receipt of the next interrupt. If an interrupt is detected, control passes to 308 where the packet corresponding to the shadow packet is located. As previously stated, the associated primary packet can be located either at the beginning of the active buffer or the end of the inactive buffer depending upon the way the system headend arranges outgoing packets. In other embodiments, a DMA register can be read at the time of the interrupt and this information used to pinpoint the location within the primary buffers that defines a location where the shadow packet resided within the original incoming data stream with respect to the primary packets. The search for the corresponding packets can then be limited to one or two packets before or after this point.

<u>Specifying packets to process</u>

Once the packet corresponding to the shadow packet is located, a new packet is generated at 312 with the primary PID and the shadow packet's payload. The new packet is then inserted in place of the shadow packet's corresponding packet in the program data stream at 318. Control then returns to 304 to await the next interrupt.

Thus, a method and apparatus for reconstituting packetized data streams representing a television program when the program uses multiple packet identifiers (PID) as in selective encryption schemes is provided. Transmission of

multiple sets of system information (SI) is avoided by incorporating a lookup table within a private data packet. This is accomplished at the headend by constructing a program association table (PAT) that associates programs with primary PIDs and constructing a plurality of program map tables (PMT), one for each program in the PAT. A lookup table is constructed to map at least one primary PID to at least one shadow PID and the PAT, the PMTs and the lookup table are then broadcast over the content delivery medium. The PAT and lookup table are then used in the STB to program PID filters and demultiplexers to handle both primary and shadow PIDs.

Software method to process PID pairs

A dual buffer arrangement in the set-top box provides ease of reconstitution of a data stream by generation of an interrupt upon receipt of a packet with a shadow PID. The buffers are toggled as a result of the interrupt and a corresponding packet can be found either at the beginning of the newly active buffer or the end of the inactive buffer. The stream of packets representing a program can then be reconstituted by creation of a new packet having the primary PID and shadow packet's payload.

While this invention has been described in terms of a cable television system and set-top boxes, equivalent satellite systems and television receivers that directly decode digital television are also contemplated and do not depart from this invention.

Those skilled in the art will recognize that the present invention has been described in terms of exemplary embodiments based upon use of a programmed processor. However, the invention should not be so limited, since the present invention could be implemented using hardware component equivalents such as special purpose hardware and/or dedicated processors which are equivalents to the invention as described and claimed. Similarly, general purpose computers, microprocessor based computers, micro-controllers, optical computers, analog computers, dedicated processors and/or dedicated hard wired logic may be used to construct alternative equivalent embodiments of the present invention.

Those skilled in the art will appreciate that the program steps and associated data used to implement the embodiments described above can be implemented using disc storage as well as other forms of storage such as for example Read Only Memory (ROM) devices, Random Access Memory (RAM) devices; optical storage elements, magnetic storage elements, magneto-optical storage elements, flash memory, bubble memory, core memory and/or other equivalent storage technologies without departing from the present invention. Such alternative storage devices should be considered equivalents.

The present invention, as described in embodiments herein, is implemented using a programmed processor executing programming instructions that are broadly described above in flow chart form that can be stored on any suitable electronic storage medium or transmitted over any suitable electronic communication medium. However, those skilled in the art will appreciate that the processes described above can be implemented in any number of variations and in many suitable programming languages without departing from the present invention. For example, the order of certain operations carried out can often be varied, additional operations can be added or operations can be deleted without departing from the invention. Error trapping can be added and/or enhanced and variations can be made in user interface and information presentation without departing from the present invention. Such variations are contemplated and considered equivalent.

While the invention has been described in conjunction with specific embodiments, it is evident that many alternatives, modifications, permutations and variations will become apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended that the present invention embrace all such alternatives, modifications and variations as fall within the scope of the appended claims.

What is claimed is: